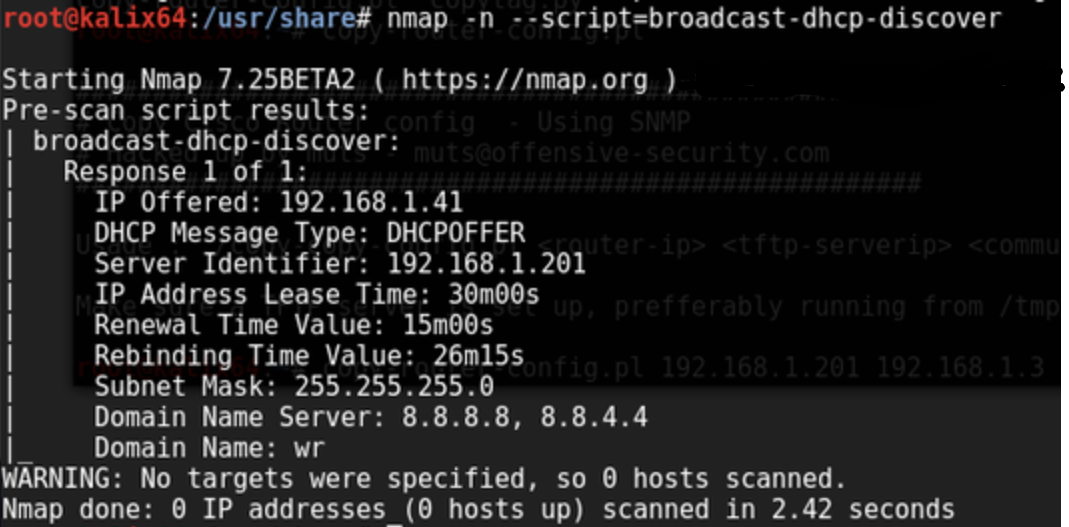
[Course | SkillFactory](https://apps.skillfactory.ru/learning/course/course-v1:SKILLFACTORY+hack_pentest+2020/block-v1:SKILLFACTORY+hack_pentest+2020+type@sequential+block@0d89ab0c393d4dc783b8d8004d61b985/block-v1:SKILLFACTORY+hack_pentest+2020+type@vertical+block@a0c189845d844dabbe37b01fb7c61fe7)

**1. Практическое задание по атакам на сетевые сервисы**

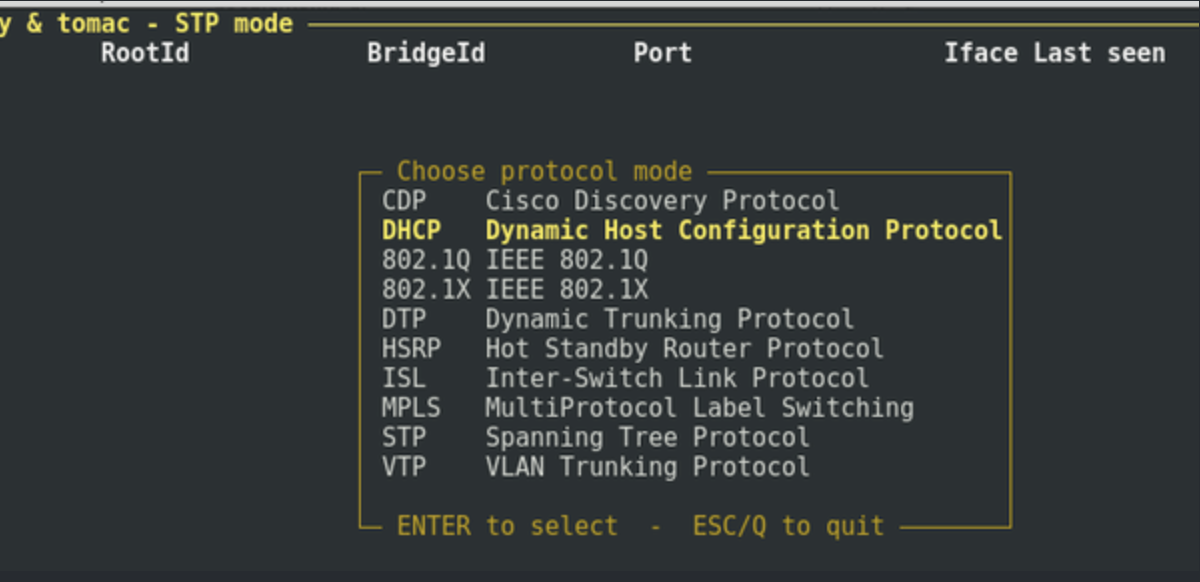
### Процесс атаки

#### Проведем атаку на переполнение пула IP-адресов DHCP сервера. Данная атака может быть использована для выведения из строя корпоративного DHCP сервера и последующая его замещение поддельным, конфигудрация которого настроена таким образом, что весь трафик новых клиентов будет проходить через хост атакующего.

#### На стороне атакующего можно выполнить скрипт nmap для обнаружения DHCP сервера в локальной сети: nmap -n --script=broadcast-dhcp-discover

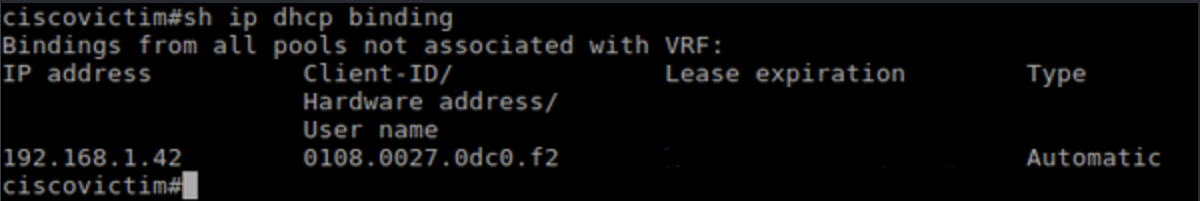
****

Запускаем Yersinia в интерактивном режиме и переходим в режим DHCP выбрав его нажатием клавиши g.

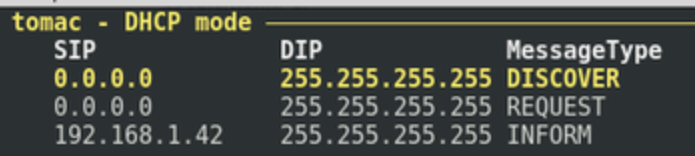


Теперь в этом режиме будут видны все DHCP пакеты, полученные Yersinia.

Проверим список выданных адресов DHCP сервера до атаки:

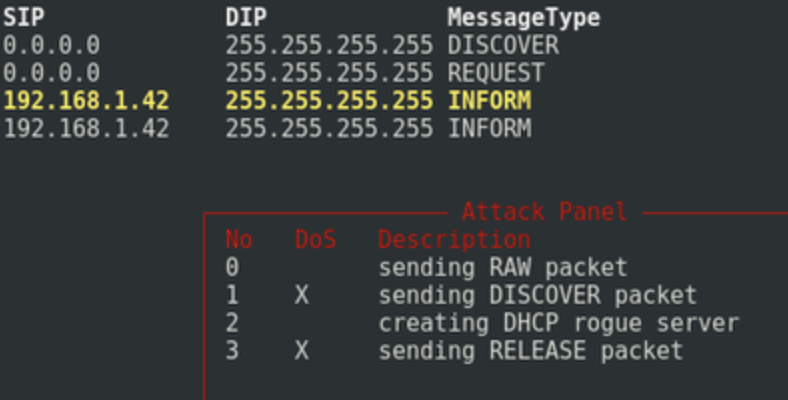


Yersinia показывает DHCP пакеты, выловленные из сети:



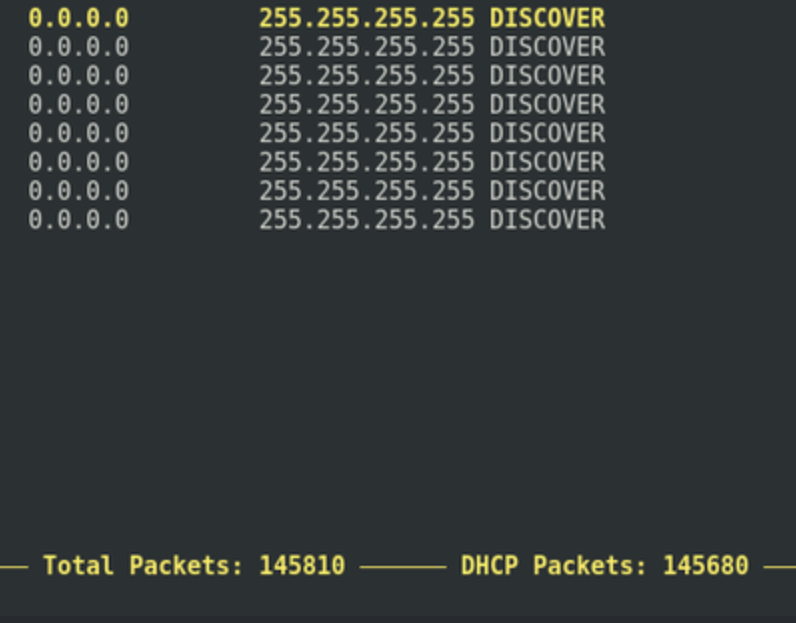
Если выбрать пакет и нажать сочетание клавиш Shift+L то можно затем при помощи атаки RAW пересылать этот пакет в сеть, или модифицировать его при помощи нажатия клавиши e – переход в режим редактирования пакета.

При нажатии на клавишу x получаем список доступных атак:

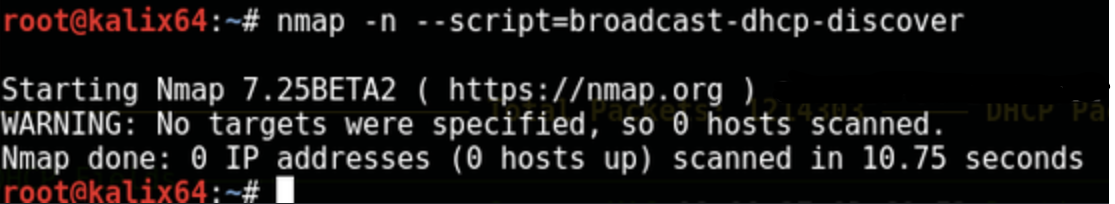


Выбираем 1

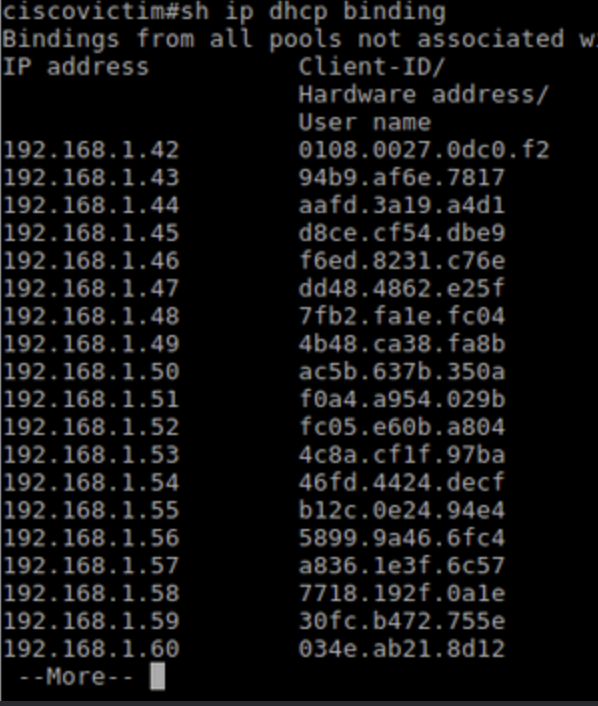
Видим, что начинает отправлять огромное количество DHCP Discover запросов:



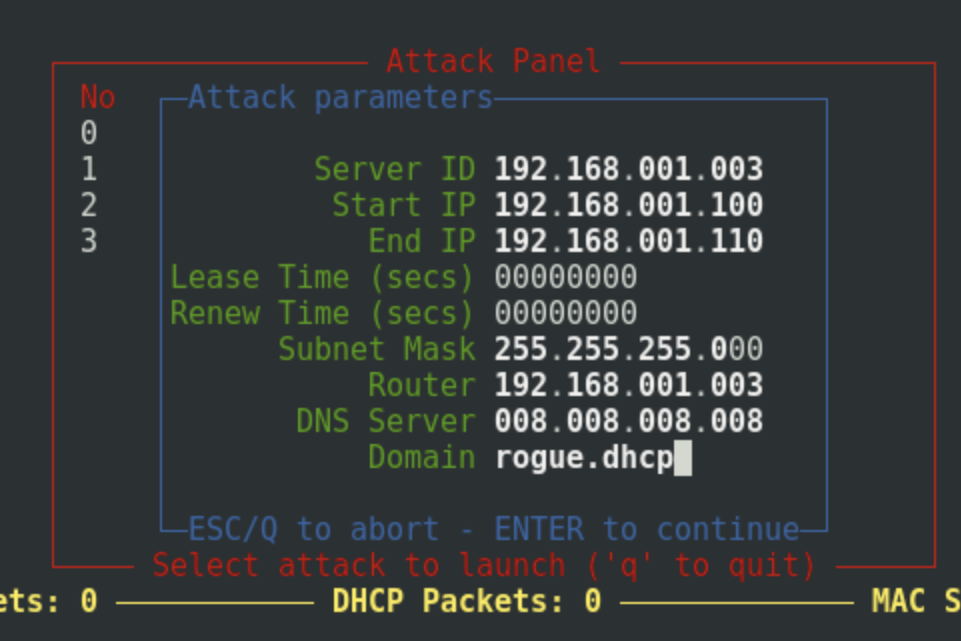
Nmap больше не показывает доступных DHCP серверов в сети. Коропоративный DHCP сервер выведен из строя.



Проверим таблицу выданных IP-адресов на роутере:



Далее вы можете запустить атаку Rogue DHCP в Yersinia, либо при помощи модуля Metasploit или любым другим способом.



Атаку на истощение пула IP адресов DHCP сервера можно также провести при помощи инструмента DHCPig. При помощи Yersinia можно проводить атаки и на другие популярные протоколы, такие как STP (Spanning Tree Protocol) и HSRP (Hot Standby Router Protocol), которые также позволят прослушивать трафик в сети.